

What is claimed is:

- 5 1. An electronic data storage apparatus for storing electronic data, comprising:
- key management means for managing an individual key unique to the electronic data storage apparatus to which said means belongs, and a common key shared with other electronic data storage apparatuses; and
- 10 encryption means for performing an encrypting process on electronic data stored in the electronic data storage apparatus to which said means belongs using the individual key, and performing an encrypting process using the common key or with data verification on electronic data transmitted to or received from
- 15 another electronic data storage apparatus.
2. The apparatus according to claim 1, wherein said key management means manages a group key as the common key to be shared in a group of a plurality
- 20 of electronic data storage apparatuses.
3. The apparatus according to claim 1, wherein:
- a main electronic data storage apparatus exists in the group;
- 25 said encryption means of said main electronic

data storage apparatus generates an individual key of each electronic data storage apparatus in the group using an individual key of the apparatus to which said means belongs; and

5 said generated individual key is distributed to each electronic data storage apparatus belonging to the group.

4. The apparatus according to claim 2, wherein:

10 a main electronic data storage apparatus exists in the group;

 said encryption means of said main electronic data storage apparatus generates a group key to be shared in the group using an individual key of the apparatus to which said means belongs; and

15 said generated group key is distributed to each electronic data storage apparatus belonging to the group.

20 5. The apparatus according to claim 2, wherein:

 a main electronic data storage apparatus exists in the group;

 said encryption means of said main electronic data storage apparatus generates a group key to be shared in the group with a key preliminarily assigned

09332477.060899

Q' conit

0609

10

15

20

25

7. The apparatus according to claim 2, wherein

said key management means manages, in addition to said group key as the common key, a public key for use in transmitting electronic data to and receiving

it from an electronic data storage apparatus belonging to a group different from a group of the electronic data storage apparatus to which said means belongs.

5 8. ~~The apparatus according to claim 1, wherein
said individual key is preliminarily assigned to
each electronic data storage apparatus before use of
the apparatus.~~

10 9. The apparatus according to claim 1, wherein:
said encryption means generates the individual
key with a key preliminarily set before use of the
apparatus to which said means belongs with a new
externally specified key; and

15 said key management means manages the generated
individual key.

20 10. The apparatus according to claim 1, wherein
said key management means manages, in addition
to the individual key and the common key, a master key
to be shared by all electronic data storage
apparatuses.

25 11. The apparatus according to claim 10, wherein:
said encryption means generates the individual

5

10

15

20

25

said key management means manages a group key as the common key depending on a hierarchical level of

a group containing the electronic data storage apparatus to which said means belongs.

14. The apparatus according to claim 13, wherein:

in the hierarchical structure of the electronic data storage apparatuses, an electronic data storage and management apparatus for managing electronic data storage apparatuses in a lower order group exists in a group at one level higher than the lower order group;

said encryption means of said electronic data storage and management apparatus generates a group key for the lower order group using the individual key of the apparatus to which said means belongs; and

said generated group key is distributed to the electronic data storage apparatuses in the group at one level lower.

15. A method of managing electronic data in an electronic data storage apparatus in a hierarchical structure having a group of a plurality of electronic data storage apparatuses as one hierarchical level, comprising the steps of:

a transmitting electronic data storage apparatus in one hierarchical level of the hierarchical

A²
cor 4

09327477-060899

structure re-encrypting data, encrypted using an individual key which is unique to and stored in the apparatus, using a higher order group key corresponding to the hierarchical level, and transmitting the re-encrypted data to an electronic data storage and management apparatus for managing the electronic data storage apparatuses in a group at one hierarchical level lower;

said electronic data storage and management apparatus for managing a lower group of electronic data storage apparatuses verifying the received data using the higher order group key;

re-encrypting the electronic data using the lower order group key corresponding to one hierarchical level lower if the electronic data is correct as a result of the verification, and transmitting the data to a receiving electronic data storage apparatus in the group at one level lower;

said receiving electronic data storage apparatus verifying received data using the lower order group key; and

re-encrypting and storing received data using an individual key unique to the apparatus if the electronic data is correct as a result of the verification.

003347-050899

A²
Bent

16. A method of managing electronic data in an electronic data storage apparatus in a hierarchical structure having a group of a plurality of electronic data storage apparatuses as one hierarchical level, comprising the steps of:

a transmitting electronic data storage apparatus in one hierarchical level of the hierarchical structure re-encrypting data, encrypted using an individual key which is unique to and stored in the apparatus, using a lower order group key corresponding to the hierarchical level, and transmitting the re-encrypted data to a lower order group electronic data storage and management apparatus for managing the electronic data storage apparatuses in the group;

said electronic data storage and management apparatus for managing a lower group of electronic data storage apparatuses verifying the received data using the lower order group key;

re-encrypting the electronic data using the higher order group key corresponding to one hierarchical level higher if the electronic data is correct as a result of the verification, and transmitting the data to a receiving electronic data storage apparatus in the group at one level higher;

said receiving electronic data storage apparatus

Q2
CGrit

002247-060899

verifying received data using the higher order group key; and

re-encrypting and storing received data using an individual key unique to the apparatus if the electronic data is correct as a result of the verification.

17. A method of storing electronic data in an electronic data storage apparatus for storing the electronic data, comprising the steps of:

communicating electronic data using a common key shared with other electronic data storage apparatuses; and

performing an encrypting process using an individual key unique to an electronic data storage apparatus on data to be stored in the electronic data storage apparatus.

18. The method according to claim 17, wherein

said electronic data storage apparatus stores as the common key a group key shared in one group of a plurality of electronic data storage apparatuses;

a transmitting electronic data storage apparatus transmits electronic data after re-encrypting using the group key the data stored in the apparatus and

00000000-00000000

A2
cont

5 when the electronic data is correct according to
a result of the verification, said electronic data is
re-encrypted using the individual key and stored.

10 said electronic data storage apparatus belonging
to a group of electronic data storage apparatuses
stores as the common key a public key of an electronic
data storage apparatus belonging to another group of
a plurality of electronic data storage apparatuses;

15 a transmitting electronic data storage apparatus
transmits electronic data after re-encrypting using
the public key the data stored in the apparatus and
encrypted using the individual key;

20 verifies the received electronic data using a private
key which is a pair to the public key; and

5 verifying stored electronic data using an
individual key unique to the electronic data storage
apparatus; and

10

15

re-encrypting the electronic data using an individual key unique to the electronic data storage apparatus and storing the data when a result of the verification is correct.

20

add 3